Welcome to the PIA for FY09!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

(FY 09) PIA: System Identification

Program or System Name:	LAN-2009
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-01-01-01-1040-00

Description of System / Application / Program:	The LAN system is comprised of network devices, workstations, terminals, servers, printers, and other devices which support communications, to include routers, hubs, switches, firewalls, etc. The LAN includes magnetic tape drives, disk drives, and uninterruptible power supplies (UPS). Access to the system is via workstations operating on Windows-family operating systems (OS) including Windows XIP and thin client terminals located throughout the medical center. Microsoft windows client workstations connect over a TCIP/IP network and may use terminal emulation software and the Remote Procedure Call (RPC) Broker to connect to other systems, such as VistA. There is access from the local LAN to
Facility Name:	VA Long Beach Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Melissa M. Ottem	(562) 826-8000	Melissa.Ottem@va.gov

Information Security Officer:	Raul A. Quiroga	(562) 826-8000	Raul.Quiroga@va.gov
Chief Information Officer:	Rodney A. Sagmit	(562) 826-8000	Rodney.Sagmit@va.gov
Person Completing Document:	Raul A. Quiroga	(562) 826-8000	Raul.Quiroga@va.gov
Other Titles:	Gerardo Cardenas	(562) 826-8000	Gerardo.Cardenas@va.gov
Other Titles:			
Other Titles:			
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	09/2007		
Date Approval To Operate Expires:	08/2011		

What specific legal authorities authorize this program or system:	The system is used in support of major application VistA in accordance with title 38, U.S. code, section 7301 (a).
What is the expected number of individuals that will have their PII stored in this system:	NONE
Identify what stage the System / Application / Program is at:	Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	15 years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	

Date of Report (MM/YYYY): 04/2009

If answers 'Yes' to one or more of the following, please check the appropriate box, continue to the next tab, and complete the remaining questions on this form. If none have been checked then skip to Signatures tab, obtain the appropriate signatures, and submit this document.

- ☐ Has a PIA NOT been completed within the last three years?
- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☐ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☐ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☐ Does this system/application/program collect, store or disseminate the SSN?

(FY 09) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?	Yes
if the answer above is no, please skip to row 16.	
For each applicable System(s) of Records, list: 1. All System of Record Identifier(s) (number): 2. Name of the System of Records: 3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	
Is PII collected by verbal methods?	
Is PII collected by automated methods?	
Is a Privacy notice provided?	
Proximity and Timing: Is the privacy notice provided at the time of data collection?	
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	

(FY 09) PIA: Notice

Please fill in each column for the data types selected.

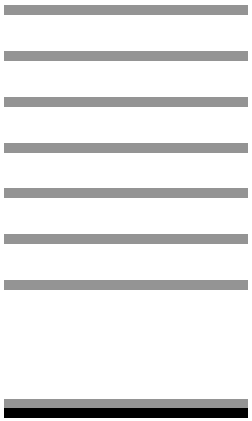
Data Type	Collection Method	What will the subjects be told about the information collection?	How is this messaged conveyed to them?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal		Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database		Written
Service Information	Electronic/File Transfer		Verbally
Medical Information	VA File Database		
Criminal Record Information	VA File Database		
Guardian Information	Verbal		
Education Information	Verbal		
Benefit Information	VA File Database		
Other (Explain)	Verbal	next of kin and emergency contact	Verbally

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)			

Family Relation (spouse, children, parents, grandparents, etc)
Service Information
Medical Information
Criminal Record Information
Guardian Information
Education Information
Benefit Information
Other (Explain)
Other (Explain)
Other (Explain)

How is a privacy notice provided?
Verbally
Written
Written
Written

Additional Comments



(FY 09) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization		No			
Other Veteran Organization		No			
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY09) PIA: Access to Records

Does the system gather information from another system?	No
Please enter the name of the system:	
Does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☐ Submitted in Person ☐ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY09) PIA: Secondary Use

Will PII data be included with any secondary use request?	No
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)
Describe process for authorizing access to this data. Answer: The Privacy Act and VA policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.	

(FY 09) PIA: Program Level Questions

Does this PIA contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Data is collected electronically based on the automation of VA forms and clinical procedures.

How is data checked for completeness?

Answer: Data is reviewed by staff and compared to paper forms.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Clinical data is not removed. Administrative data is updated with each application for care.

How is new data verified for relevance, authenticity and accuracy?

Answer: New data is compared with printed form or via patient verification.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 09) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA Records Control Schedule 10-1.

Explain why the information is needed for the indicated retention period?

Answer:

What are the procedures for eliminating data at the end of the retention period?

Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA Records Control Schedule 10-1, Item XLIII, 2.b. (page 190). At the present time, VistA Imaging retains all images. We are performing a study to explore whether some images can be eliminated on an earlier schedule.

Where are these procedures documented?
Answer: VA Handbook 6300; Record Control Schedule 10-1

How are data retention procedures enforced?
Answer: VA Records Control Schedule 10-1 (page 8).

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 09) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No

If Yes, How will parental or guardian approval be obtained?

Answer:

FY 09: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 09) PIA: Final Signatures

Facility Name: VA Long Beach Healthcare System

Title:	Name:	Phone:	Email:
Privacy Officer:	Melissa M. Ottem	(562) 826-8000 X 2244	Melissa.Ottem@va.gov
Information Security Officer:	Raul A. Quiroga	(562) 826-8000 X 3234	Raul.Quiroga@va.gov
Chief Information Officer:	Rodney A. Sagmit	(562) 826-8000 X 5637	Rodney.Sagmit@va.gov
Person Completing Document:	Raul A. Quiroga	(562) 826-8000 X 3234	Raul.Quiroga@va.gov
System / Application / Program Manager:	Gerardo Cardenas	(562) 826-8000 X 5572	Gerardo.Cardenas@va.gov

Signature not verified! MELISSA OTTEM Digital Signature Block
Digitally signed by: MELISSA OTTEM
DN: CN = MELISSA OTTEM O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff
Date: 2009.04.09 13:32:13 -08'00'
Reason: I have reviewed this document

Signature not verified! RAUL A QUIROGA Digital Signature Block
Digitally signed by: RAUL A QUIROGA
DN: CN = RAUL A QUIROGA O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff
Date: 2009.04.09 08:48:16 -08'00'
Reason: I have reviewed this document

Signature not verified! RODNEY A SAGMIT Digital Signature Block
Digitally signed by: RODNEY A SAGMIT
DN: CN = RODNEY A SAGMIT O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff
Date: 2009.04.09 14:29:14 -08'00'
Reason: I have reviewed this document

Signature not verified! RAUL A QUIROGA Digital Signature Block
Digitally signed by: RAUL A QUIROGA
DN: CN = RAUL A QUIROGA O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff
Date: 2009.04.09 08:51:41 -08'00'
Reason: I have reviewed this document

Signature not verified! GERARDO CARDENAS Digital Signature Block
Digitally signed by: GERARDO CARDENAS
DN: CN = GERARDO CARDENAS O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff
Date: 2009.04.09 10:45:02 -08'00'
Reason: I have reviewed this document

Date of Report: 4/1/2009

OMB Unique Project Identifier	029-00-01-01-01-1040-00
Project Name	LAN-2009